Introductie tot de cursus

Introductie tot de cursus

Voordat u begint met het bestuderen van de cursus Security en IT willen wij u in deze introductie informeren over de bedoeling van de cursus, de opzet van het cursusmateriaal en de werkwijze die wij van u verwachten. U vindt hier nog geen studiestof, maar praktische en studietechnische informatie die u kan helpen bij het studeren.

1 De functie van de cursus

Het vakgebied security kent vele facetten, die niet alleen techniek maar ook zaken als menselijk gedrag, ethiek, management en beheer bestrijken. In deze cursus richten we ons vrijwel volledig op technische informatica-aspecten van security. We schenken aandacht aan uiteenlopende onderwerpen: cryptografie, access control, malware, en de beveiliging van besturingssystemen, netwerken, het world wide web en databases. Centraal daarbij staan vragen als: welke kwetsbaarheden zijn er, welke aanvallen zijn daardoor mogelijk, welke maatregelen zijn er vooraf om aanvallen te voorkomen en achteraf om geslaagde aanvallen te detecteren, en welke beperkingen kennen deze maatregelen.

De cursus maakt deel uit van de bacheloropleidingen Informatica en Informatiekunde en van het schakelprogramma voor de masteropleidingen Computer Science en Software Engineering (als voorbereiding voor de mastercursus Software Security). Daarnaast is de cursus ook interessant voor 'losse' cursisten die meer willen weten over de beveiliging van computersystemen, zonder een volledige informatica-opleiding te volgen.

2 De inhoud van de cursus

2.1 VOORKENNIS

Als voorkennis voor deze cursus wordt kennis van minstens één programmeertaal verondersteld, alsmede globale kennis van computernetwerken, internetprotocollen, besturingssystemen en relationele databases. De cursus bevat korte introducties tot computernetwerken, internetprotocollen, besturingssystemen en relationele databases. Deze dienen om uw kennis op te frissen of bij te spijkeren, maar ze zijn ontoereikend als u nog volledig onbekend bent met deze onderwerpen.

Als u een opleidingsstudent bent, beschikt u over voldoende voorkennis als u de propedeuse hebt afgerond en bij voorkeur ook de cursus Besturingssystemen. Als losse cursist moet u de voorkennis op andere wijze hebben opgedaan. De hoeveelheid wiskunde in de cursus is minimaal gehouden; kennis op havoniveau is voldoende. Het gebruikte cursusmateriaal is voor een groot deel Engelstalig. U dient het Engels in voldoende mate te beheersen om de cursus te kunnen bestuderen.

2.2 LEERDOELEN VAN DE CURSUS

De leerdoelen omschrijven welke kennis, inzichten en vaardigheden u door het bestuderen van de cursus wordt geacht te verwerven.
We verwachten dat u na het bestuderen van de cursus:
– de betekenis kent van termen als confidentiality, integrity, availability, assurance, authenticity en anonymity
– bedreigingen, aanvallen en security-principes voor computersystemen kunt benoemen
– verschillende access-controltechnieken kent en de werking ervan globaal kunt uitleggen
– de beginselen van cryptografie kent en globaal de werking van moderne cryptografische algoritmen en toepassingen daarvan kunt uitleggen
– kunt uitleggen welke beveiligingspolicies en -maatregelen in besturingssystemen worden toegepast
– de werking van diverse vormen van malware kunt beschrijven en kunt aangeven welke bescherming daartegen mogelijk is
– diverse bedreigingen en beveiligingsmaatregelen voor netwerken, internetprotocollen en webapplicaties kent en globaal kunt uitleggen hoe ze werken
– bekend bent met security-aspecten van databases.

2.3 OPBOUW VAN DE CURSUS

De cursus is verdeeld in dertien leereenheden. Leereenheid 1 geeft een introductie tot computersecurity waarin basisconcepten en -principes aan de orde komen. Leereenheid 2 is gericht op access control met daarin verschillende modellen voor toegangscontrole. De leereenheden 3 en 4 geven een inleiding in de cryptografie. Leereenheid 5 bevat een practicum waarin de cryptografische algoritmen uit leereenheid 3 en 4 worden geïllustreerd. In leereenheid 6 en 7 kijken we nader naar de security van besturingssystemen en in leereenheid 8 naar verschillende vormen van malware. De leereenheden 9 en 10 zijn gewijd aan security van internetprotocollen. Leereenheid 11 bevat een practicum waarin u de aanvallen en beveiligingsmaatregelen die in leereenheid 9 en 10 aan de orde zijn geweest, zelf kunt uitproberen in een virtuele omgeving. U gaat daarbij niet alleen aan de slag met het implementeren en configureren van beveiligingsmaatregelen, maar ook kunt u als hacker zelf aanvallen uitvoeren en de effecten daarvan bestuderen. In leereenheid 12 kijken we nader naar de security van het world wide web. Tot slot behandelen we in leereenheid 13 security-aspecten van databasesystemen.

De cursus heeft een omvang van 4,3 studiepunten, wat overeenkomt met een bruto studielast van 100 tot 120 uur. Voor het bestuderen van de leerstof in de leereenheden hebt u circa 75 uur nodig. De resterende tijd is hoofdzakelijk bedoeld voor het bijwonen van de online begeleidingsbijeenkomsten, het bekijken van de cursussite in de elektronische leeromgeving, het installeren van de software die in de practica wordt gebruikt, de tentamenvoorbereiding via herhalen van de leerstof en het maken van de eindtoets en oefententamens, en tot slot het tentamen.

2.4 LEERMIDDELEN

Het schriftelijke cursusmateriaal bestaat uit het werkboek, dat u momenteel leest, en het tekstboek 'Introduction to Computer Security', Pearson New International Edition, van Michael Goodrich en Roberto Tamassia uit 2014. Het werkboek beschrijft welke delen van het tekstboek u moet bestuderen, en geeft aanvullingen, toelichtingen, opgaven en de uitwerkingen daarvan.

In het werkboek vindt u slechts een summiere beschrijving van de practica in leereenheid 5 en 11. De concrete opdrachten die u in de practica uitvoert, vindt u op de cursussite in de elektronische leeromgeving. Daar vindt u ook de software, alsmede informatie over de installatie en het gebruik ervan, die u in de practica nodig hebt.

Op de cursussite vindt u ook actuele mededelingen, errata, een discussiegroep, informatie over de online begeleidingsbijeenkomsten, de eindtoets en twee oefententamens.

3 Gebruiksaanwijzing

3.1 TEKSTBOEK EN WERKBOEK

Leereenheid

De cursus is verdeeld in leereenheden. Een *leereenheid* is een afgerond deel van de stof, dat betrekking heeft op een hoofdstuk of een deel van een hoofdstuk uit het tekstboek. Het werkboek voegt in elke leereenheid de volgende ingrediënten toe aan de stof van het tekstboek:
– een korte inleiding op de betreffende stof
– leerdoelen die aangeven wat u na het bestuderen van de leereenheid moet weten en/of kunnen
– studeeraanwijzingen, waarin wordt aangegeven welke delen van het betreffende hoofdstuk uit het tekstboek bestudeerd moeten worden en een aanduiding van de geschatte studielast
– waar nodig aanvullingen, toelichtingen en errata bij het tekstboek
– opgaven
– een zelftoets, waarmee u kunt nagaan of u de leerdoelen van de leereenheid hebt bereikt
– een terugkoppeling op de opgaven en de zelftoets; wij raden u aan niet meteen het antwoord in de terugkoppeling op te zoeken. U leert meer en beter als u eerst zelf een oplossing probeert te vinden.

Nummering

De nummering van de leereenheden volgt niet de nummering van de hoofdstukken in het tekstboek. In elke leereenheid wordt duidelijk aangegeven welke delen van welk hoofdstuk uit het tekstboek bestudeerd moeten worden.

Hoofdstuk

Het tekstboek bevat 10 *hoofdstukken*, zoals aangegeven op pagina 1 van het tekstboek. Deze hoofdstuknummering wordt echter verderop in het tekstboek niet meer getoond. Kijk als voorbeeld naar pagina 1 van het tekstboek. Daar wordt alleen de hoofdstuktitel 'Introduction' vermeld, zonder hoofdstuknummer. Aan het begin van elk hoofdstuk geeft het tekstboek de inhoudsopgave van dat hoofdstuk. De onderdelen van een hoofdstuk duiden we aan als *secties* en *subsecties*. Bijvoorbeeld, sectie 1 van hoofdstuk 1 is getiteld 1 'Fundamental Concepts'. Deze sectie heeft vier subsecties: 1.1 'Confidentiality, Integrity, and Availability', 1.2 'Assurance, Authenticity, and Anonymity', 1.3 'Threats and Attacks' en 1.4 'Security Principles'.

Secties en subsecties

Bestudering van tekstboek

Sommige hoofdstukken bestudeert u in zijn geheel, van andere hoofdstukken kunt u onderdelen overslaan. Als dat laatste het geval is, wordt dit uitdrukkelijk vermeld in de studeeraanwijzingen in het werkboek. Aan het begin van elke leereenheid wordt bij 'Studeeraanwijzing' aangegeven welke secties van een hoofdstuk al dan niet tot de leerstof horen. Als u subsecties kunt overslaan, wordt dat aan het begin van de betreffende sectie in detail vermeld.
Het werkboek vermeldt expliciet elke sectie die bestudeerd moet worden. Meestal geeft het werkboek ook extra informatie en opgaven bij die sectie, incidenteel wordt alleen als studeeraanwijzing vermeld dat deze sectie uit het tekstboek ook tot de leerstof behoort. De subsecties van een te bestuderen sectie worden daarentegen niet allemaal expliciet in het werkboek genoemd. Dat gebeurt alleen als er iets bij een subsectie opgemerkt wordt.
In leereenheid 1 wordt bijvoorbeeld expliciet aangegeven dat sectie 1.1 'Confidentiality, Integrity, and Availability' tot de leerstof behoort. Aangezien het werkboek verder geen studeeraanwijzingen over de subsecties geeft, behoren alle subsecties van deze sectie tot de leerstof. Deze sectie heeft drie subsecties: 'Confidentiality', 'Integrity' en 'Availability'. In het werkboek worden alleen de subsecties 'Confidentiality' en 'Availabiliy' expliciet genoemd. Subsectie 'Integrity' wordt niet expliciet vermeld, maar behoort dus wel tot de leerstof.

Wij raden u aan bij het bestuderen van het tekstboek het werkboek bij de hand te houden en per sectie te kijken of er studeeraanwijzingen, toelichtingen, enzovoort zijn. Wilt u om welke reden dan ook het tekstboek bestuderen zonder dat u steeds het werkboek raadpleegt, dan is het raadzaam vooraf in het werkboek na te gaan of er eventueel onderdelen vervallen.

Kernbegrippen

Studeer-aanwijzingen

Iedere pagina in het werkboek heeft aan de linkerkant een marge, waarin studeeraanwijzingen en kernbegrippen worden getoond. *Kernbegrippen* zijn centrale begrippen en worden cursief gedrukt als ze nader uitgelegd worden. *Studeeraanwijzingen* zijn aanwijzingen of onderdelen wel of niet bestudeerd moeten worden, hoe de tekst gelezen moet worden, herhalingen of verwijzingen naar andere leereenheden, enzovoort. Studeeraanwijzingen worden niet-cursief in de marge vermeld.

Studeeraanwijzing

Dit is een voorbeeld van een studeeraanwijzing.

Leestekst

Soms is een facultatieve passage ingevoegd die nader op de stof ingaat of een kanttekening plaatst. Een dergelijke passage behoort niet tot de tentamenstof en is een *leestekst.*

Een leestekst wordt afgedrukt in kleine letters, waarvan hier een voorbeeld.

Weblink

In het werkboek wordt incidenteel verwezen naar bronnen op internet of op de cursussite door middel van de tekst weblink in de marge.

3.2 STUDIEBEGELEIDING

Als u zich inschrijft voor deze cursus, krijgt u toegang tot de cursussite in de elektronische leeromgeving. Daar vindt u onder andere contactgegevens van de docent en een discussiegroep waarin u vragen kunt stellen en opmerkingen kunt maken over de cursus, waarop de docent reageert. Medestudenten kunnen desgewenst ook reageren.

Eenmaal per studiejaar vindt een reeks online begeleidingsbijeenkomsten plaats. In deze bijeenkomsten licht de docent de leerstof op hoofdlijnen toe, kunt u vragen stellen over de leerstof, worden extra opgaven behandeld, en wordt aandacht besteed aan het tentamen. Nadere informatie over deze bijeenkomsten kunt u vinden op de cursussite.

3.3 TENTAMEN

De cursus wordt afgesloten met een regulier schriftelijk tentamen dat bestaat uit een aantal open vragen. De tentamendata kunt u vinden in de studiegids en op de cursussite.

U hebt voor het tentamen drie uur de tijd. Het is niet toegestaan bij het tentamen het cursusmateriaal of ander materiaal te gebruiken. Wel is het gebruik van een rekenmachine toegestaan.

Op de cursussite vindt u een eindtoets en twee oefententamens. (Deze oefententamens zijn twee tentamens die daadwerkelijk afgenomen zijn bij de cursus.) Met behulp daarvan kunt u zich aan het eind van de cursus voorbereiden op het tentamen.

3.4 PRACTICA

De cursus bevat twee practica die in leereenheid 5 en 11 worden beschreven. De opdrachten in deze practica kunt u individueel uitvoeren op uw eigen computer. De benodigde software, de opdrachtbeschrijvingen en de uitwerkingen van de opdrachten, vindt u op de cursussite. U hoeft de uitwerkingen van de opdrachten niet in te leveren en deze tellen dus ook niet mee in het eindcijfer van de cursus.

Het practicum in leereenheid 5 illustreert cryptografische technieken. Het practicum in leereenheid 11 is gewijd aan netwerk security. Een goede manier om inzicht te krijgen in de kwetsbaarheden en beveiliging van computersystemen is door ervaring op te doen en zelf voor luistervink te spelen, zelf aanvallen uit te voeren, en zelf tools te gebruiken om die aanvallen te voorkomen of op zijn minst te detecteren. Een probleem daarbij is dat het vaak gaat om technieken en tools waarvan het gebruik strafbaar is of zou kunnen worden, of niet op prijs wordt gesteld door de organisatie waartegen ze worden toegepast. Om deze redenen maken we in leereenheid 11 gebruik van een virtuele omgeving waarin u enkele van de genoemde ervaringen kunt opdoen. De virtuele omgeving is opgebouwd uit software die u op uw eigen pc kunt installeren via de cursussite. In de virtuele omgeving kunt u een computernetwerk bouwen en verschillende aspecten van beveiliging bekijken en uitproberen. Zo kunt u aanvallen uitvoeren en maatregelen implementeren om die aanvallen op te merken of te voorkomen.
Wij willen u er met nadruk op wijzen dat het gebruik van deze technieken en tools op het publieke internet of een intranet strafbaar kan zijn of op zijn minst niet op prijs kan worden gesteld door derden. Wij verzoeken u daarom dringend deze niet toe te passen buiten de virtuele omgeving.